EXTENDED SMART CARD SYSTEM AND ITS CONTROL METHOD

Publication number: KR20030049387
Publication date: 2003-06-25
Inventor: KIM SUNG WOO (KR); SEO WON IL (KR)
Applicant: KIM SUNG WOO (KR); NCBIZ CO LTD (KR); SEO WON IL (KR)
Classification:
- international: ***G06K19/07;*** **G06K19/07;** (IPC1-7): G06K19/07
- European:
Application number: KR20010079581 20011214
Priority number(s): KR20010079581 20011214

Abstract of **KR20030049387**

PURPOSE: An extended smart card system and its control method are provided to enable a user to access various data and applications, stored at a large sized storage of a server, by using a smart card. CONSTITUTION: The system comprises a smart card(10), a card reader(12), a host PC(14), and a server(18). The smart card(10) stores card data, e.g. a user ID, a password, and some applets. The card reader(12) reads the card data if the smart card is inserted into a slot. The host PC(14), electrically connected to the card reader(12), stores the read card data at a temporary memory, and transmits the read data to an external system over a network. The server(18) checks an access right by using the transmitted card data, transmits an access permission signal to the host PC(14), and allots a virtual storage for the accessing smart card.

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.[7]
G06K 19/07

(11) 공개번호 특2003-0049387
(43) 공개일자 2003년06월25일

(21) 출원번호 10-2001-0079581
(22) 출원일자 2001년12월14일

(71) 출원인 엔시비즈(주)
서울특별시 강남구 삼성동 162-24 아리빌딩 5층

김성우
경기 성남시 분당구 이매동 아름마을태영아파트 307동 901호

서원일
서울특별시 양천구 목동 902 목동아파트 219동 502호

(72) 발명자 김성우
경기 성남시 분당구 이매동 아름마을태영아파트 307동 901호

서원일
서울특별시 양천구 목동 902 목동아파트 219동 502호

(74) 대리인 김준효

심사청구 : 있음

(54) 확장 스마트 카드 시스템 및 그 제어 방법

요약

본 발명은 확장 스마트 카드 시스템 및 그 제어 방법에 관한 것으로서, 사용자의 아이디(ID)와 패스워드(PASSWORD) 및 소정의 애플릿(APPLET) 등의 카드데이터를 저장하고 있는 스마트카드(SMART CARD)와; 상기 스마트카드가 삽입되면 상기 스마트카드의 카드데이터를 읽어들이는 카드리더(CARD READER)와; 상기 카드리더와 전기적으로 연결되어 상기 스마트카드로 부터 읽어들인 카드데이터를 임의의 기억장소에 저장하고 이를 외부에 연결되는 네트워크(NETWORK)를 통해 외부로 송신하는 호스트피씨(HOST PC); 및 상기 호스트피씨로부터 송신된 카드데이터를 수신받아 상기 스마트카드의 접근권한이 정당한지를 판단하여 정당한 권한이 있으면 허가신호를 네트워크를 통해 상기 호스트피씨로 전송하고, 자체에 상기 스마트카드의 가상 스토리지(VIRTUAL STORAGE)를 할당하는 서버(SERVER);를 포함하여 구성되는 것을 특징으로 한다.

대표도

도 1

색인어

스마트카드, 카드리더, 호스트피씨, 서버

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 확장 스마트 카드 시스템의 구성도이고,

도 2는 스마트카드와 카드리더 및 호스트피씨의 하드웨어 연결구성도이고,

도 3은 본 발명에 따른 스마트카드의 확장 개념도이고,

도 4는 본 발명에 따른 스마트카드를 일반 드라이브로 인식하는 방법을 도시한 흐름도이고,

도 5는 본 발명에 따른 스마트카드를 가상 스토리지로 인식 프로토콜의 개념도이고,

도 6은 본 발명에 따른 호스트피씨의 어플리케이션과 서버의 통신 개념도이고,

도 7은 본 발명에 따른 호스트피씨의 어플리케이션과 스마트카드의 통신 개념도이며,

도 8은 스마트카드의 서버 스토리지 접근 권한에 대한 개념도이다.

* 도면의 주요부분에 대한 부호의 설명 *

10 : 스마트카드, 12 : 카드리더, 14 : 호스트피씨, 16 : 네트워크, 18 : 서버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 확장 스마트 카드 시스템 및 그 제어 방법에 관한 것으로, 더욱 구체적으로 설명하면, 스마트카드를 이용하여 확장된 솔루션을 제공할 수 있는 시스템에 관한 것이다.

일반적으로 스마트카드는 크레디트 카드와 크기가 같으나, 플라스틱 내에 임베디드 전자회로를 통하여 정보를 저장하고 처리할 수 있다. 최근에는 칩 기술과 암호화의 약진으로, 스마트카드는 더욱 강력해진 기능을 바탕으로 지폐를 대신하여 전자캐쉬를 가능하게 했고, 개인의 진료 기록을 안전하게 저장하고, 케이블과 위성 방송에 대한 승인되지 않은 접근을 차단하며, 그리고 무선전화의 보안을 개선하는데 까지 사용된다. 이미 유럽 그리고 아시아에서 매우 일반적인 스마트카드는 e-business 분야에 있는 보안과 저장장치 테크놀로지에 대한 늘어나는 요구로 많은 분야에서 중요한 자리를 차지하기 시작했다.

그러나, 이러한 다양한 분야에서 스마트 카드 시스템의 도입에 대한 필요성에도 불구하고 스마트카드 내의 메모리인 이이피롬(EEPROM)의 용량 한계로 인해 스마트카드를 사용하는 사용자는 자신이 필요로 하는 만큼의 데이터를 충분히 저장할 수 없는데 가장 큰 문제점이 있다.

발명이 이루고자 하는 기술적 과제

따라서, 이러한 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은 사용자들이 그들의 편의와 휴대용으로서 스마트카드를 디스켓이나 시디롬 같은 휴대용 미디어 솔루션으로서 스마트카드를 사용할 수 있도록 하는 시스템을 제공하는데 있다. 본 발명의 다른 목적은 스마트카드를 거대한 저장장치처럼 사용하여, 바이러스 백신같은 데이터와 어플리케이션 프로그램을 제공하는 것을 희망한다.

본 발명의 또 다른 목적은 카드 발행인이나 어플리케이션 공급자들이 그들의 카드 사용자를 위한 업데이트된 일반적인 어플리케이션 라이브러리를 제공하고 이를 사용자가 사용할 수 있는 시스템을 제공하는데 있다.

발명의 구성 및 작용

본 발명은 스마트카드를 이용한 확장 시스템 및 그 방법에 관한 것으로서, 사용자의 아이디(ID)와 패스워드(PASSWORD) 및 소정의 애플릿(APPLET) 등의 카드데이터를 저장하고 있는 스마트카드(SMART CARD)와; 상기 스마트카드가 삽입되면 상기 스마트카드의 카드데이터를 읽어들이는 카드리더(CARD READER)와; 상기 카드리더와 전기적으로 연결되어 상기 스마트카드로 부터 읽어들인 카드데이터를 임의의 기억장소에 저장하고 이를 외부에 연결되는 유무선 네트워크(NETWORK)를 통해 외부로 송신하는 호스트피씨(HOST PC); 및 상기 호스트피씨로부터 송신된 카드데이터를 수신받아 상기 스마트카드의 접근권한이 정당한지를 판단하여 정당한 권한이 있으면 허가신호를 유무선 네트워크를 통해 상기 호스트피씨로 전송하고, 자체에 상기 스마트카드의 가상 스토리지(VIRTUAL STORAGE)를 할당하는 서버(SERVER); 를 포함하여 구성되는 것을 특징으로 한다.

상기 스마트카드의 애플릿은 상기 서버에 그 에플릿에 대응하는 범용 데이터 및 어플리케이션(APPLICATION)이 저장되어 상기 호스트피시로 부터 읽기/쓰기/실행 (READ/WRITE/EXECUTION) 등의 명령이 수행되면 상기 서버의 범용 데이터 및 어플리케이션(APPLICATION)이 수행되는 것을 특징으로 한다.

상기 스마트카드의 애플릿들은 읽기/쓰기가 가능한 이이피롬에 저장되는 것을 특징으로 한다.

상기 호스트피씨는 일반 PC인 것을 특징으로 한다.

상기 호스트피씨는 피디에이(PDA)인 것을 특징으로 한다. 상기 호스트피씨는 이동전화단말기인 것을 특징으로 한다.

상기 호스트피씨는 신용카드 단말기인 것을 특징으로 한다.

상기 스마트카드는 RF card, VOP platform, MULTOS , Windows for Smart Card 등의 접촉식 또는 비접촉식 카드 중에 어느 하나인 것을 특징으로 한다.

상기 카드리더는 상기 호스트피씨와 유에스비포트(USB PORT)를 통해 전기적으로 연결하여 구성함이 바람직하다.

상기 카드리더는 상기 호스트피씨의 키보드에 내장되어 전기적으로 연결하여 구성함이 바람직하다.

상기 카드리더는 상기 호스트피씨와 컴포트(COM PORT)를 통해 전기적으로 연결하여 구성함이 바람직하다.

상기 호스트피씨의 데이터의 복사시에 실시간 또는 데이터전송 완료 직후에 바이러스 체크하는 것을 특징으로 한다.

본 발명은 (a) 사용자가 스마트카드를 카드리더에 삽입하는 단계;

(b) 상기 단계(a)의 스마트카드의 삽입에 따라 호스트피씨의 특정 어플리케이션이 수행되는 단계;

(c) 상기 단계(b)로 부터 카드리더의 카드데이터를 읽어들이는 단계;

(d) 상기 단계(c)로 부터 읽어들인 카드데이터를 서버에 전송하는 단계;

(e) 상기 단계(d)로 부터 전송된 카드데이터를 상기 서버에서 확인하는 단계;

(f) 상기 단계(e)로 부터의 확인데이터를 상기 호스트피씨로 전송하는 단계;

(g) 상기 단계(e)로 부터 전송된 확인데이터에 따라 스마트카드를 상기 호스트피씨의 일반 드라이브로 인식하여 사용하는 단계;를 포함하여 구성된다.

상기 단계(g)는 상기 스마트카드에 데이터 및 어플리케이션을 저장하면 해당 애플릿이 상기 스마트카드에 저장되고 실제 데이터 및 어플리케이션은 상기 서버의 스토리지에 저장되는 단계인 것을 특징으로 한다.

본 발명에 따른 확장 스마트 카드 시스템 및 그 제어 방법을 첨부한 도면을 참고로 하여 이하에 상세히 기술되는 실시예에 의하여 그 특징들을 이해할 수 있을 것이다.

도 1은 본 발명에 따른 확장 스마트 카드 시스템의 구성도이고, 도 2는 스마트카드와 카드리더 및 호스트피씨의 하드웨어 연결구성도이고, 도 3은 본 발명에 따른 스마트카드의 확장 개념도이고, 도 4는 본 발명에 따른 스마트카드를 일반 드라이브로 인식하는 방법을 도시한 흐름도이고, 도 5는 본 발명에 따른 스마트카드를 가상 스토리지로 인식 프로

토콜의 개념도이고, 도 6은 본 발명에 따른 호스트피씨의 어플리케이션과 서버의 통신 개념도이고, 도 7은 본 발명에 따른 호스트피씨의 어플리케이션과 스마트카드의 통신 개념도이며, 도 8은 스마트카드의 서버 스토리지 접근 권한에 대한 개념도이다.

도 1에 따라 확장 스마트 카드 시스템을 설명하면 다음과 같다.

확장 스마트 카드 시스템은 스마트카드(10), 카드리더(12), 호스트피씨(14) 및 상기 호스트피씨(14)에 네트워크(16)에 의해 연결되는 서버(18)로 구성된다.

스마트카드(10)는 카드소유자의 아이디(ID)와 패스워드(PASSWORD) 및 서버(16)내의 스토리지(20)에 저장되어 있는 데이터 및 어플리케이션에 대한 애플릿이 저장되어 있다.

한편, 상기 애플릿은 특정 플래폼에 사용되는 고유명사가 아닌 통상의 카드 내의 어플리케이션을 지칭한다.

카드리더(12)는 상기 스마트카드가 삽입되어 있으면 상기 스마트카드의 데이터인 아이디, 패스워드 및 애플릿 등의 소정의 카드데이터를 전기적으로 연결되어 있는 호스트피씨(14)에 전송하거나 반대로 호스트피씨(14)의 데이터를 스마트카드 (10)로 전송하게 되는 정보의 통로역할을 하게 된다.

호스트피씨(14)는 상기 스마트카드(10)를 일종의 저장매체인 확장된 드라이브로 인식하여 이를 하나의 거대한 저장장소처럼 사용하게 된다. 데이터를 스마트카드(10)에 복사하면 애플릿 만이 생성되고 실제 저장되어야 하는 데이터는 스마트카드(10)가 아니라 호스트피씨(14)와 네트워크(16)로 연결되어 있는 서버(18)에 할당되는 스마트카드(10)를 위한 스토리지(20)에 저장되는 것이다. 상기 서버(18)는 스마트카드(10)의 소유자를 위한 데이터 및 어플리케이션을 저장하기 위한 스토리지(20)가 할당되어 있고 상기 스마트카드(10)의 데이터 및 어플리케이션이 수행되면 그에 따라 상기 서버(18)의 데이터가 호스트피씨(14)로 송수신되거나 수행되는 것이다.

도 2에 따라 조금 더 상세히 스마트카드(10)와 카드리더(12) 및 호스트피씨 (14)의 구성을 살펴보면 다음과 같다.

스마트카드(10)는 입출력되는 데이터를 연산하는 중앙처리장치(CPU)(22)와 그 내부에 데이터연산시 임시 데이터 저장을 위한 램(RAM)(24), 카드의 동작을 위한 시스템프로그램이 저장되는 롬(ROM)(26), 그리고 전원이 차단되어도 기억된 정보가 지워지지 않는 비휘발성이며 전원이 투입되어 소정의 정보를 읽기 쓰기가 가능하여 카드소유자의 아이디, 패스워드 및 소정의 애플릿 정보가 저장되는 이이피롬(EEPROM)(28)으로 구성된다. 이와같이 구성되는 스마트카드(10)를 카드리더(12)의 소켓(30)에 삽입하면 카드리더(12) 내에 소켓(30)과 전기적으로 연결되는 커넥 터1(32)와 호스트피씨(14)와 연결되는 케이블(34)을 통해 호스트피씨의 커넥터2(36)와 연결되는 스마트카드 콘트롤러(38)로 데이터의 송수신이 이루어 진다. 스마트카드 콘트롤러(38)를 통해 수신되는 데이터는 호스트피씨의 메인 프로세서(Main Processor)(40)에서 연산된다.

상기와 같은 시스템 구성으로 부터 이하 스마트카드를 확장 스토리지로의 사용예를 설명한다.

도 3의 확장 개념도에 따르면, 확장 스마트카드 포털 솔루션(eXtended Smart Card Portal Solution ; 이하 'XSCP' 라고 한다)(100)은 스마트카드(10)의 버추얼 이이피롬의 확장을 가능하게 한다. 피씨를 위한 개인 데이터 또는 일반적인 어플리케이션들은 XSCP(100)를 위한 버추얼 저장장치(Virtual Storage for XSCP ; 이하 'VSX' 라고 한다)(102)에 저장될 수 있으며, 그 각각의 에플릿(104)들은 VSX(102)안에 그들의 데이터를 저장할 수 있다.

VSX(102)는 네트워크를 통하여 필요한 권한이 주어지며, 스마트카드(10)에서 가상 스토리지는 실제로 서버 저장장치의 일부분이다.

VSX(102)는 사용자가 파일을 탐색할 때 스마트카드(10)에 저장하는 처럼 보이지만 그것은 네트워크를 통하여 서버의 스토리지에 연결된다.

즉, VSX(102)는 파일안에 씨디롬과 같은 드라이브처럼 사용하므로 사용자들은 서버 저장장치가 스마트카드(10) 안에 있는 스토리지라고 생각하게 된다. 스마트카드(10)의 애플릿(104)은 오직 약간의 정보, 예를 들면 접근 제어를 위한 데이터인 아이디, 패스워드 등을 가지고 있다. 상술한 바와 같이, 만약 개인용 컴퓨 터(PC)가 네트워크에 연결된다면, 그들은 편리하게 스마트카드(10)를 거대한 디스켓이나 읽기/쓰기(read/write)가 가능한 시디롬(CDROM)처럼 사용할 수 있으므로 스마트카드(10) 안에서 유일한 포털 사이트(Portal Site)를 위해 XSCP(100)를 확장하여 사용함이 바람직하다. 상기 XSCP(100)는 스마트카드(10)의 애플릿(104)과 한쌍의 호스트피씨 어플리케이션들을 제공하며, 이를 이용하면 많은 애플릿(104)과 쌍으로 존재하는 피씨(PC)의 어플리케이션은 쉽게 분산이 가능하고, 사용자는 VSX(102) 안의 아이콘을 단지 클릭하므로서 애플릿/호스트피씨(applet/HostPC) 어플리케이션을 인스톨(Install)한다. 아울러, 그것은 업데이트(update)된 범용 피씨 어플리케이션들과 주식 정보, e-book들 및 영화 등의 유용한 데이터

를 제공받는 것이 가능하다.

도 3 내지 도 6에 따라 스마트카드를 일반 드라이브로 인식하는 방법을 살펴보면 다음과 같다.

스마트카드(10)가 원래 작은 컴퓨터 시스템이므로, XSCP(100)는 확장 스토리지로 간단히 디자인되어 파일탐색기로 서버(18)의 스토리지(20)와 통신하는 것을 가능하게 했으며, 이는 사용자에게는 스마트카드(10)안의 스토리지와 같이 보이는 것이 가능하게 되었다. 스마트카드(10)의 애플릿(104)은 적은 데이터 즉, 개인의 ID, 패스워드, 파일과 디렉토리를 위한 접근 특권을 포함한다.

스마트카드(10)를 카드리더에 삽입하면(200), 호스트피씨(14)의 특정어플리케이션(300)이 수행(202)되어 스마트카드(10)로 부터 카드데이터인 애플릿(104)들 을 읽어들이게 된다(204).

따라서, 호스트피씨(14)의 어플리케이션(300)은 스마트카드(10)로 부터 이러한 데이터를 읽어들이고(204), 그리고 네트워크를 통해 서버(18)에 전송한다 (206). 아이디, 패스워드 그리고 그것의 특권이 맞으면 서버(18)는 결정한다(208). 그리고 그 결과신호를 호스트피씨(14)의 어플리케이션(파일 탐색기안의 드라이브 심벌을 만들고 그리고 서버 저장장치에 맵핑되어있는)에 전송(210), 즉 응답을 하는 것이다

상기와 같은 조건이 만족되면, 스마트카드(10)를 저장매체인 카드드라이브로 인식하고 사용이 가능하게 된다(212).

사용자가 어떤 파일을 이 스마트카드(10) 드라이브에 복사할 때, 그 호스트피씨 어플리케이션(300)은 데이터를 서버(18)에 보내고 전송(폴더부터 폴더까지 보통의 파일 복사처럼 파일 탐색기 상의 파일심벌들을 표시하는)을 완료한다.

파일을 바이러스로 부터 보호하기 위해 전송된 각각의 파일은 실시간으로 또는 나중에 바이러스 백신에 의해 체크되도록 구성함이 바람직하다.

그러나 이것은 실행 시간이나 전송 시간의 지체를 야기할 수 있으므로 큰 파일은 나중에 일괄 처리되도록 체크되어야 하고, 중요한 작은 파일들은 실시간으로 체크되도록 구성함이 바람직하다.

도 7은 서버의 스토리지 접근 권한에 대한 개념도이다.

사용자(400)는 VSX(102)안에 있는 자신의 폴더인 개인 데이터 스토리지 (Storage for Personal Data, 이하 'SPD'라고 한다)(402)에 데이터를 저장한다. 사 용자(400)는 그 폴더의 읽기/쓰기/실행(read/write/execute) 권한을 가지므로 사용자(400)는 데이터(어플리케이션들을 포함하여)를 저장하고 지우고, 물론 데이터나 파일을 읽고 수행한다. 그 영역은 사용자(400) 사이에 분리될 것이고, 그리고 사용자(400)는 다른 사용자의 데이터를 접근할 수 없어야 하므로 사용자(400)의 활동과 사적인 자료는 완전히 숨겨진다. 즉, VSX(102)안의 사용자들(400, 401) 자신의 폴더나 디렉토리는 그 사용자에게 모든 권한을 정식으로 인가받는다.

비록 XSCP(100)가 버추얼 확장 저장을 위하여 시작될 지라도, 가장 큰 기능들 중에 하나는 인터넷 포털 사이트처럼, XSCP는 컨텐츠들과 같은 범용 데이터들과 어플리케이션들(General Data and Applications, 이하 'GDA'라고 한다)(404)을 분배하고 공유하는 것이다. 이 또한 폴더나 디렉토리처럼 보이지만 사용자는 단지 읽기/실행(read/execute) 권한을 가진다. 오직, XSCP 관리자(408)만이 쓰기/업데이트 (write/update) 권한을 가진다. 이렇게 함으로써, 자료를 지울 수 있는 위험을 배제할 수 있다.

어떤 데이터 또는 어플리케이션들은 특수한 사용자에게 보일 수 있으나, 일반적인 사용자는 볼 수 없다. 스마트카드 기술에 관련된 가장 큰 특징 중에 하나는 멀티 어플리케이션 환경을 지원하는 것이며 이는 카드안에 인스톨되기 위한 많은 카드 애플릿들이 인에이블된다. 이와 같은 경우, 카드 발행인은 애플릿들과 키 메니지먼트(key management)의 분산를 위한 스마트카드관리시스템(SmartCard Manage ment Systems; SCMS)을 제공해야 한다. 이것이 애플릿들의 자료실(Morgue Of Applets 이하 'MOA'라고 한다)(406)이다. 이들 애플릿들의 폴더나 디렉토리는 사용 자들(400, 401)에 의해서 지워지거나 변경되어지지 않고 오직 XSCP 관리자(408)만이 권한을 가진다. 또한, 인스톨을 위해 어플리케이션이 필요하므로 애플릿 인스톨은 어떤 키들을 가진 인스톨 도구에 의해 처리되어야 한다. 이 키들은 카드 발행인들이나 어플리케이션 공급자들에게 제공되고 이 인스톨 툴은 카드 플랫폼들 예를들면, VOP(Visa Open Platform), MULTOS(the platform announced by MasterCard)) 그리고 Windows for smart card 들에 따라 다르다. 이러한 툴들은 일반 어플리케이션처럼 XSCP에 의해 제공될 수 있으며, 일단 그 툴은 사용자의 PC에 설치되고, 사용자는 단지 한번의 클릭으로 자신의 카드에 VSX안의 카드 에플릿들을 인스톨하는 것이 가능하다.

접근 제어 특권(Access Control Privilege 이하 'ACP'라고 한다)은 XSCP에서 가장 중요한 기술 중에 하나인데 이를 사용하면, 모든 사용자들(400, 401)은 읽기/쓰기/실행/업데이트(read/write/execute/update) 허가와 같은 모든 특권을 가지는 그들 자신만의 저장장치를 가질 수 있다. 어떤 영역은 특별 사용자에게 보여야 한다, 그리고 어떤 부분은 X

SCP 관리자(408)를 제외한 모든 사용자들(400, 401)에는 읽기(read)만이 가능해야 한다. 한편, 컴퓨터에 사용되는 이진 정보(binary information)라는 것은 항시 복사가 가능한 정도가 아니라 복사된 것도 원본과 동일하므로 원본과 복사본의 차이가 전혀 없다.

따라서, 본 발명은 프로그램의 복사가 불가능한 어떤 물리적인 키(KEY)가 있어야만 동작하도록 만들고 있다.

여기에 사용되는 물리적인 키라는 것은 여러가지가 될 수 있는데, 암호를 담 고 있는 디스켓이나 프린터 포트에 꽂는 하드웨어 장치, 지문이나 음성 인식장치뿐만 아니라 오리지날 CD(Original CD)자체도 물리적인 키로서의 역할을 할 수 있다. 이러한 물리적인 키는 어떤 특정한 초기화가 수행되지 않으면 소프트웨어가 실행되지 않게 해주는 가드 모듈(Guard module)이라고 불리는 특수한 코드를 삽입함으로서 복사가 불가능하도록 만든다.

가드 모듈은 물리적인 키를 찾아내어 만약 이 키가 존재한다면 프로그램 실행에 필요한 초기화를 수행하게 된다.

간단하게 말하자면, 카피 프로텍션(Copy Protection)이란 어떤 외부적인 동작(External action)에 의해 작동되도록 원래의 코드에 변화를 가하는 것이며, 가드 모듈은 물리적인 키 자체이거나 혹은 물리적인 키를 인식할때 필요한 동작을 제공한다.

모든 복사방지장치는 다음의 세가지 요소로 구성되어 있으며 어느 한가지라도 빠지게 되면 동작하지 않게 된다.

외부 동작에의 의존성(Dependency on External Action)

오리지널 소프트웨어는 가드 모듈이 동작하지 않으면 실행되지 않도록 어떠한 방법으로든 변형되어야만 하는데,

보통 소프트웨어 내의 가드 모듈을 호출(Calls to the guard module)하는 방법으로 구성되나 소프트웨어 초기화의 가장 좋은 방법은 이런 동작을 암호화하는 것이다.

즉, 암호화(Encryption)란 코드의 파장을 바꾸어서 실행되지 않도록 하거나 더이상 인식불가능하도록 만드는 것을 의미한다.

가드 모듈(The Guard Module)

가드 모듈은 특정한 방법으로 소프트웨어를 실행가능하도록 복구하는 역할을 하는 코드로 하여금 소프트웨어를 초기화 시켜 실행 가능하도록 해준다.

즉, 물리적인 키가 존재할때에만 이러한 동작을 수행하고, 키가 인증되어 가드 모듈이 동작하면 소프트웨어를 초기화 시키고 실행한다.

이러한 키의 인식 및 소프트웨어를 실행가능하도록 복구하는 기능외에, 가드모듈은 그 자신의 동작을 완전히 감추고 실행되는 것이 특징이다.

또한, 키가 없을 때, 키가 동작하는 것처럼 속이는 어떤 트릭이나 키의 복사가 불가능해야 할 뿐만 아니라, 가드 모듈이 어떻게 동작하는지도 완벽히 숨겨져야 하는데 이러한 것을 코드 보안(Code security)이라고 부른다. 가드모듈 자체는 특정한 방법, 암호화와 디버깅-트래핑(Encryption and debug-trapping)으로 보호되어 있고, 소프트웨어가 키 없이는 동작하지 않도록 한다.

물리적인 키(The Physical key)

물리적인 키는 사용자가 프로텍션된 소프트웨어를 소유하고 있다는 혹은 사용권을 가지고 있다는 증거가 되는 실제의 물리적인 장치이다.

한편, 스마트카드외에 피디에이(PDA)를 일반 드라이브로 인식하여 확장 스토 리지로의 사용을 할 수 있다. 또한, 피디에이(PDA)의 또 다른 강력한 장점은 VSX(102)안에 있는 자신의 폴더인 개인 SPD(402)에 데이터가 저장된 서버와 연결되어 동기화(Synchronization) 된다는 점이다. 즉, VSX(102)와 피디에이가 연결 됨으로써 모든 데이터가 피디에이와 VSX(102) 2곳에 저장되게 되며 어느 한 곳의 데이터가 변동되더라도 동기화 기능을 이용하여 다른 쪽의 데이터도 자동으로 변환되는 것이다. 또한, 피디에이와 VSX(102)를 연결하여 입력된 정보들의 수정, 추가, 백업을 지원함으로써, 새로운 차원의 개인정보관리 방안을 제시한다.

이상과 같이 본 발명의 실시예에 대하여 상세히 설명하였으나, 본 발명의 권리범위는 이에 한정되지 않으며, 본 발명의 일실시예와 실질적으로 균등의 범위에 있는 것까지 본 발명의 권리범위가 미친다.

발명의 효과

이상의 설명에서 알 수 있는 바와 같이, 본 발명에 따르면 스마트카드를 한정된 크기의 이이피롬의 저장용량에 상관없이 하나의 거대한 스토리지처럼 사용할 수 있는 효과가 있다. 또한, 스마트카드 사용자만이 사용할 수 있는 자신만의 저장장치를 가지므로 스마트카드시스템이 구성되어 있는 어떤 환경에서도 사용이 가능한 효과가 있다.

아울러, 서버의 스토리지에 저장되어 있는 데이터 및 어플리케이션에 다양한 접근 권한을 부여함으로서 서버관리자의 입장에서는 효율적인 서버관리가 가능한 효과가 있다.

(57) 청구의 범위

청구항 1.
사용자의 아이디(ID)와 패스워드(PASSWORD) 및 소정의 애플릿(APPLET) 등의 카드데이터를 저장하고 있는 스마트카드(SMART CARD);

상기 스마트카드가 삽입되면 상기 스마트카드의 카드데이터를 읽어들이는 카드리더(CARD READER);

상기 카드리더와 전기적으로 연결되어 상기 스마트카드로 부터 읽어들인 카드데이터를 임의의 기억장소에 저장하고 이를 외부에 연결되는 유무선 네트워크 (NETWORK)를 통해 외부로 송신하는 호스트피씨(HOST PC); 및

상기 호스트피씨로부터 송신된 카드데이터를 수신받아 상기 스마트카드의 접근권한이 정당한지를 판단하여 정당한 권한이 있으면 허가신호를 유무선 네트워크를 통해 상기 호스트피씨로 전송하고, 자체에 상기 스마트카드의 가상 스토리지 (VIRTUAL STORAGE)를 할당하는 서버(SERVER);를 포함하여 구성되는 것을 특징으로 하는 확장 스마트카드 시스템.

청구항 2.
제 1항에 있어서,

상기 스마트카드의 애플릿은 상기 서버에 그 에플릿에 대응하는 범용 데이터 및 어플리케이션(APPLICATION)이 저장되어 상기 호스트피시로 부터 읽기/쓰기/실행 (READ/WRITE/EXECUTION) 등의 명령이 수행되면 상기 서버의 범용 데이터 및 어플리케이션(APPLICATION)이 수행되는 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 3.
제 1항에 있어서,

상기 스마트카드의 애플릿들은 읽기/쓰기가 가능한 이이피롬에 저장되는 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 4.
제 1항에 있어서, 상기 서버는 특정인에게 읽기/쓰기/실행의 모든 권한을 주어 사용이 가능하고 타사용자가 볼수없는 특정스토리지; 및

일반 사용자가 단지 읽기 권한만 가지고 볼수 있으며, 특정관리자만이 쓰기 /업데이트가 가능한 읽기전용스토리지;로 구성되는 되는 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 5.
제 1항에 있어서, 상기 서버에는 어떤 외부적인 동작에 의해 작동되되, 원래의 코드에 변화를 가하도록 물리적인 키 자체이거나 혹은 물리적인 키를 인식할때 필요한 동작을 제공하는 것을 특징으로 하여 소프트웨어 불법 복제를 방지하는 확장 스마트 카드 시스템.

청구항 6.
제 1항에 있어서, 상기 호스트피씨는 일반 PC인 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 7.
제 1항에 있어서, 상기 호스트피씨는 피디에이(PDA)인 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 8.
제 1항에 있어서, 상기 호스트피씨는 이동전화단말기인 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 9.
제 1항에 있어서, 상기 호스트피씨는 신용카드 단말기인 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 10.
제 1항에 있어서, 상기 가상 저장공간을 데이터 변환의 용도로 사용할 수 있는 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 11.
제 1항에 있어서, 상기 스마트카드는 RF card, VOP platform, MULTOS , Windows for Smart Card 등의 접촉식 또는 비접촉식 카드 중에 어느 하나인 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 12.
제 1항에 있어서, 상기 호스트피씨의 데이터의 복사시에 실시간 또는 데이터전송 완료 직후에 바이러스 체크하는 것을 특징으로 하는 확장 스마트 카드 시스템.

청구항 13.
제 1항에 있어서, 상기 호스트피씨와 서버 간의 데이터 통신에 있어 유선인 PSTN, PSDN, Internet 관련망, ISDN,유선 랜, TCP/IP 망, X.25망 등과 무선인 CDMA 관련망(CDMA2000, 동기식, 비동기식 포함) , 무선 랜, WAP 등의 네트워크를 통한 확장 스마트 카드 시스템.

청구항 14.
(a) 사용자가 스마트카드를 카드리더에 삽입하는 단계;

(b) 상기 단계(a)의 스마트카드의 삽입에 따라 호스트피씨의 특정 어플리케이션이 수행되는 단계;

(c) 상기 단계(b)로 부터 카드리더의 카드데이터를 읽어들이는 단계;

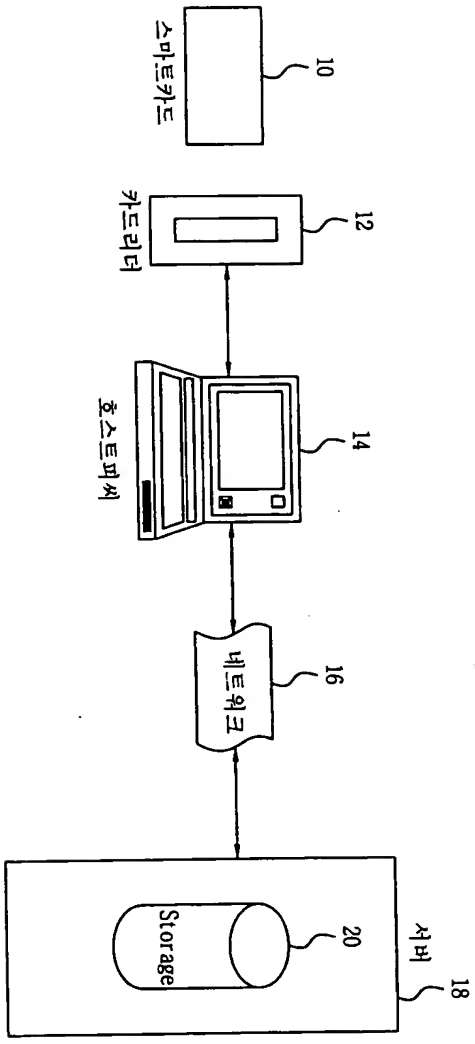
(d) 상기 단계(c)로 부터 읽어들인 카드데이터를 서버에 전송하는 단계; (e) 상기 단계(d)로 부터 전송된 카드데이터를 상기 서버에서 확인하는 단계; (f) 상기 단계(e)로 부터의 결과신호를 상기 호스트피씨의 어플리케이션으로 전송하는 단계;

(g) 상기 단계(e)로 부터 전송된 확인데이터에 따라 스마트카드를 상기 호스트피씨의 일반 드라이브로 인식하여 사용하는 단계;를 포함하여 구성되는 것을 특징으로 하는 확장 스마트 카드 제어 방법.

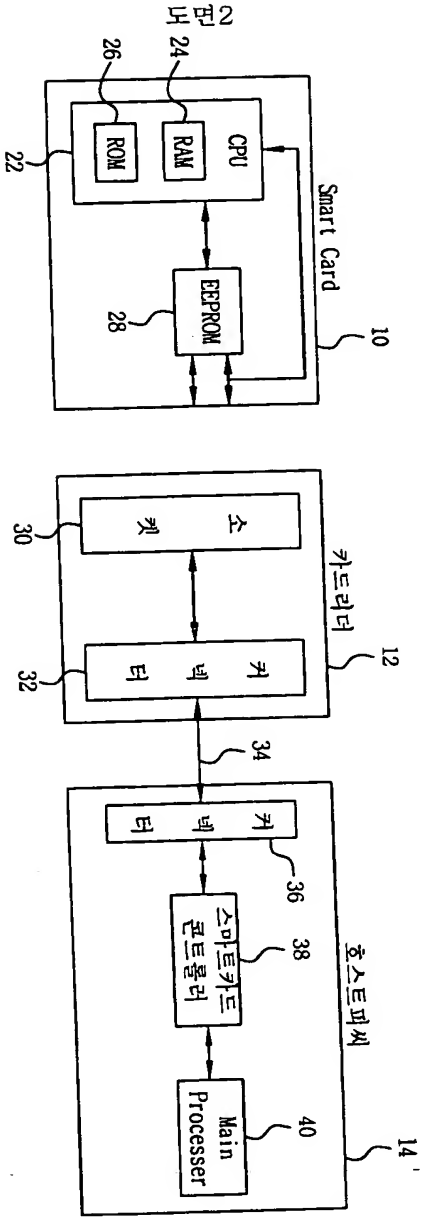
청구항 15.
제 14항에 있어서, 상기 단계(g)는 상기 스마트카드에 데이터 및 어플리케이션을 저장하면 해당 애플릿이 상기 스마트카드에 저장되고 실제 데이터 및 어플리케이션은 상기 서버의 스토리지에 저장되는 단계인 것을 특징으로 하는 확장 스마트 카드제어 방법.

도면

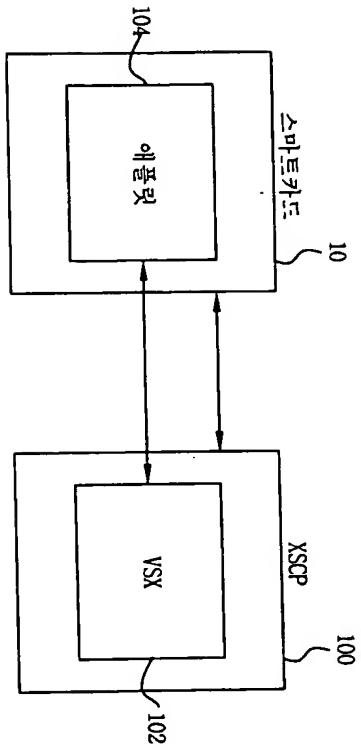
도면1



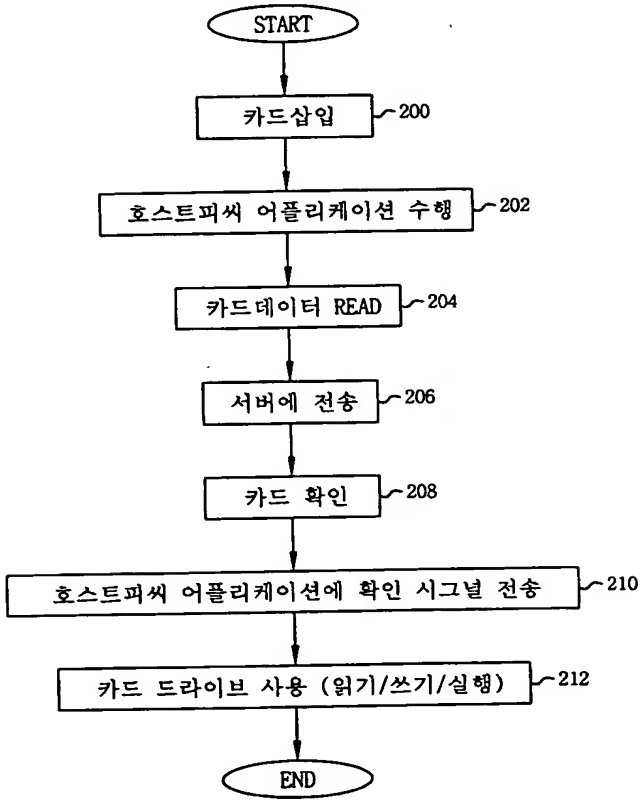
도면2


Smart Card
10
CPU
RAM
ROM
EEPROM
22
24
26
28
카드리더
12
소켓
커넥터
30
32
34
호스트피씨
14
커넥터
36
스마트카드 콘트롤러
38
Main Processer
40

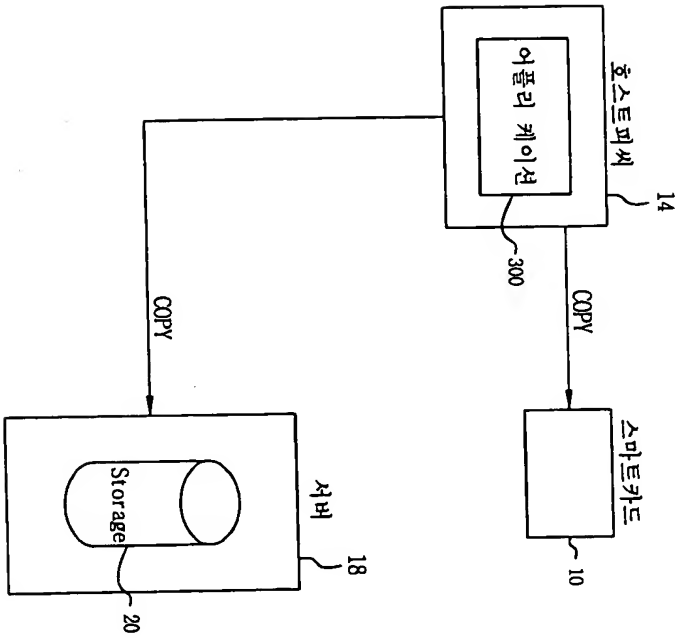
도면3


104
애플릿
스마트카드
10
VSX
XSCP
100
102

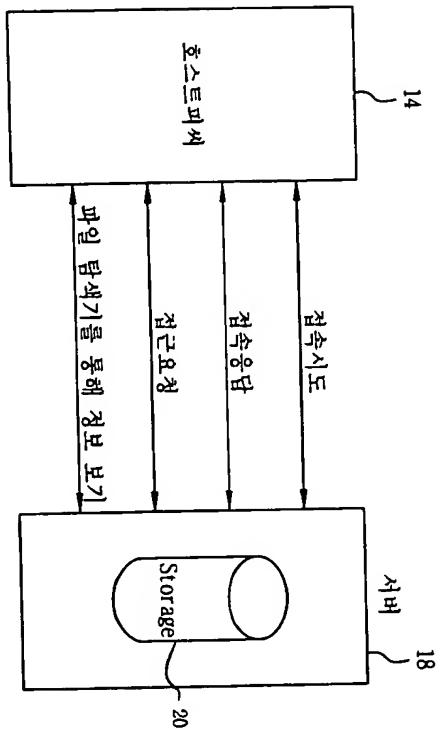
도면4


START
카드삽입
200
호스트피씨 어플리케이션 수행
202
카드데이터 READ
204
서버에 전송
206
카드 확인
208
호스트피씨 어플리케이션에 확인 시그널 전송
210
카드 드라이브 사용 (읽기/쓰기/실행)
212
END

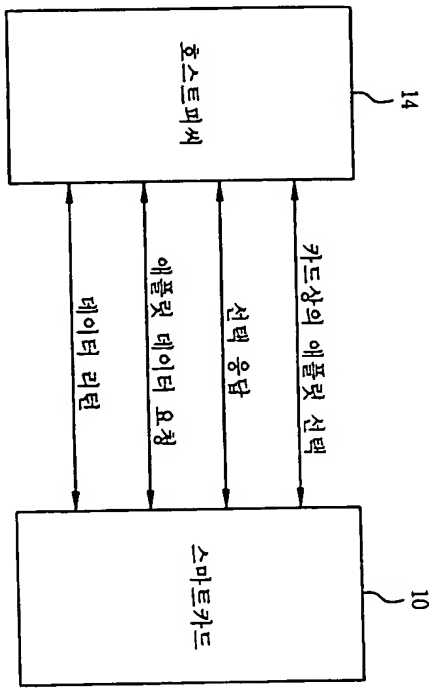
도면5


호스트피씨
14
어플리 케이션
300
COPY
COPY
스마트카드
10
서버
18
Storage
20

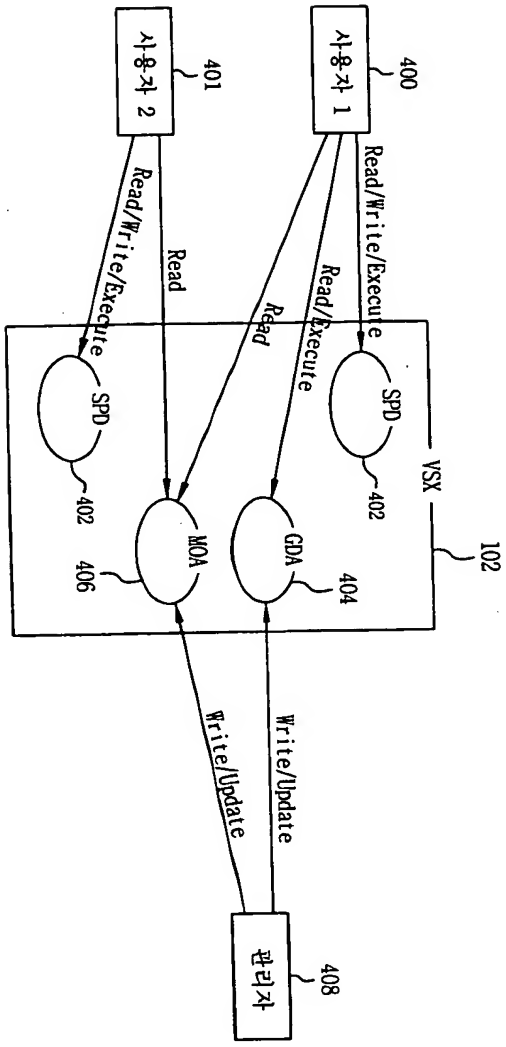
도면6


호스트피씨
14
파일 탐색기를 통해 정보 보기
접근요청
접속응답
접속시도
서버
18
Storage
20

도면7



도면8


사용자 1
400
사용자 2
401
Read/Write/Execute
Read
Read
Read/Execute
SPD
402
SPD
402
VSX
102
MOA
406
GDA
404
Write/Update
Write/Update
관리자
408